

RECEIVED
CENTRAL FAX CENTER

OCT 04 2007

Confirmation No.8281

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	BENOIT	Examiner:	Brown, C.
Serial No.:	10/084,755	Group Art Unit:	2134
Filed:	February 25, 2002	Docket No.:	PHFR 010022
Title:	COMPACT AND LOW-COST SYSTEM FOR RECEIVING SCRAMBLED SIGNALS FROM A PLURALITY OF OPERATORS		

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence and the papers, as described hereinabove, are being transmitted via facsimile-Formal Entry, to the attention of the Examiner at Commissioner for Patents, MAIL STOP Appeal Briefs P.O. Box 1450, Alexandria, VA 22313-1450, on October 4, 2007.

By: Kelly Down

Facsimile No.: 571 273-8300

REPLY BRIEF

Mail Stop Appeal Briefs
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Customer No.
65913

Dear Sir:

This Reply Brief is submitted pursuant to 37 C.F.R. § 41.41(a)(1) for the above-referenced patent application. On August 14, 2007 the Examiner provided an Examiner's Answer to Appellant's Appeal Brief submitted on May 24, 2007, in support of the Notice of Appeal filed March 29, 2007 and in response to the rejections of claims 1-10 as set forth in the Final Office Action dated December 4, 2006.

No fee should be required for the timely filing of this Reply Brief. However, if deemed necessary, authorization is given to charge/credit Deposit Account number 50-0996 (NXPS.333PA) for all required fees/overages.

RECEIVED
CENTRAL FAX CENTER

OCT 04 2007

Status of the Claims:

Claims 1-10 are pending in the application. Claims 1-10 stand rejected and are presented for appeal. No claims were previously cancelled or allowed. A complete listing of the claims under appeal is provided in an Appendix to this Brief.

Grounds of Rejection

The following grounds of rejection are presented for review:

A. Claims 1 and 10 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,115,821 to Newby, in view of U.S. Patent No. 6,912,513 to Candelore, and further in view of U.S. Patent Publication No. 2002/0001383 to Kasahara.

B. Claim 2 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Newby, in view of Candelore, further in view of Kasahara, and still further in view of U.S. Patent No. 5,029,207 to Gammie.

C. Claim 4 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Newby, in view of Candelore, further in view of Kasahara, and still further in view of "Functional Model of a Conditional Access System" by EBU Project Group (hereinafter "EBU").

D. Claim 7 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Newby, in view of Candelore, further in view of Kasahara, and still further in view of European Patent No. EP 1168137A1 to Della Valle.

Arguments

In addressing the Examiner's Answer of August 14, 2007, this Reply Brief further explains why the rationale, which is common to each of the rejections at issue, is flawed. As explained in connection with the underlying Appeal Brief's individual arguments and claim groupings (under respective headings), each such rejection relies on a combination of references (*i.e.*, Newby in view of Candelore further in view of Kasahara) that lacks the requisite motivation for skilled artisan to implement this combination. This Reply Brief presents a single argument, from more of a technical perspective, why the asserted combination of references is improper. In this regard, this Reply Brief is not intended to replace Appellant's Appeal Brief (submitted on May 24, 2007) and its respectively-presented arguments and claim groupings remain relevant and should be preserved.

The 35 U.S.C. 5 103(a) rejections of claims 1-10 are improper because there is no reason to combine the references in the manner asserted by the Examiner.

The Examiner's rejections, including the Examiner's Answer of August 14, 2007, fail to assess the consequences of the proposed combination of references with particular regard to the corresponding erroneous reason for combining the references. Appellant respectfully submits that the Examiner's reliance upon the Supreme Court's recent *KSR v. Teleflex* does not alleviate the Examiner's duty to view the references as a whole nor does it completely remove the Examiner's duty to provide a valid reason to combine the references. "... a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. ..." This is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known." *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (U.S. 2007)

Thus, merely demonstrating that various elements are independently known does not satisfy the standards articulated by the U.S. Supreme Court. In this instance, the only reason in the record for implementing the combination is the Examiner's erroneous motivation to combine. The Examiner's motivation to combine is improper because the combination of references function in a manner that contradicts the asserted motivation to combine the references.

The Examiner's asserted reason for combining the Kasahara reference with the Newby reference is to provide stronger crypto system and enhance security. The specific aspect plucked from the Kasahara reference, as applied to the Newby system, would compromise the security provided by the crypto system of the Kasahara reference. The following discussion provides a discussion of security-risks that would result from the Examiner's asserted combination. These aspects appear to have been overlooked by the Examiner. Accordingly, a more detailed discussion of the teachings of the references is necessary and reveals how unsuited the method of the Kasahara reference is to the environment of the Newby reference.

The Kasahara reference teaches a system that is capable of providing the public with an encryption mechanism (public key). Data encrypted using the public key that can only be decoded by the holder of a number of secret keys. *See, e.g., Kasahara, FIG. 1 and relevant discussion.* In practical applications, the sender of the information has no knowledge of the secret keys, and thus, neither the sender nor an intermediate nefarious party can decode the information. *See, e.g., Kasahara at paragraph 40.* As clearly taught by the Kasahara reference, the secure aspect of Kasahara's encryption technique lies in the decoder having multiple levels of secret keys that do not need to be transmitted from the sender to the receiver. *See, e.g., Kasahara at paragraphs 9-14.* This is exemplified by the paragraph (*i.e., paragraph 43*) immediately following the specific portion of Kasahara relied upon by the Examiner. At paragraph 43, Kasahara teaches that the public key (and presumably only the public key) is disclosed to the public. In view of the teachings of the Kasahara reference, the import of maintaining control of the secret keys would be paramount to the security of the encryption method.

Directly contradicting the teachings of the Kasahara reference, the Examiner's asserted combination relies upon the distribution of the secret encryption keys through the very network that is viewed as the security risk. More specifically, the Examiner's combination would transmit the secret keys using the only available network (*i.e., 27a/27b of FIG. 1*) of the Newby reference. Thus, the Examiner appears to be attempting to modify the Newby reference to transmit the secret keys of the Kasahara reference over the relatively unsecured network(s) 27a/27b. This, of course, would severely undermine the security of the Kasahara method because the secret keys would be transmitted via an unsecured network (*i.e., using the same path as the encrypted data*). Thus, the Kasahara

reference's public key encryption method is unsuited for the Newby system as the former is designed for numerous senders to transmit (public-key) encrypted data to a secure receiver and the latter is designed to transmit from a secure transmitter to numerous relatively-unsecured receivers. For at least the aforementioned reasons, the record clearly indicates that the Examiner's inverted application of the encryption method of the Kasahara reference would not be adopted by one of skill in the art because one would not use a public key at the secure transmitter while risking transmission of each of the secret keys over the unsecure portion of the system.

In view of the above argument and the underlying Appeal Brief, there is no valid reason to combine the references in the manner asserted by the Examiner. As clearly articulated by the U.S. Supreme Court in the *KSR v. Teleflex* decision, the mere identification of elements in the prior art is not sufficient to establish a proper rejection under 35 U.S.C. § 103(a). As applied to the facts of this Appeal, the only reason to combine the element that is present in the record is contradicted by the teachings of the references and the function of the asserted combination. Thus, no valid reason remains for combining the references in the manner asserted by the Examiner. Accordingly, the rejections must be reversed because there is no reason to combine the references in the manner suggested by the Examiner.

RECEIVED
CENTRAL FAX CENTER

OCT 04 2007

Conclusion

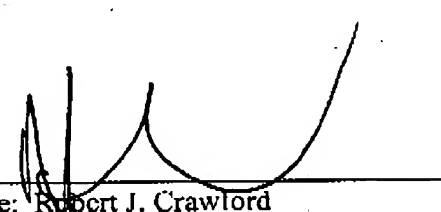
In view of the above discussion and further in view of the discussion in the above-referenced Appeal Brief, Appellant submits that the rejections of claims 1-10 are improper. Appellant therefore requests reversal of the rejections as applied to the appealed claims and allowance of the entire application.

Authority to charge the undersigned's deposit account was provided on the first page of this brief.

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131

CUSTOMER NO. 65913

By: 
Name: Robert J. Crawford
Reg. No.: 32,122
651-686-6633
(NXPS.333PA)

**RECEIVED
CENTRAL FAX CENTER****OCT 04 2007****APPENDIX OF APPEALED CLAIMS 1-10 (10/084,755)**

1. A system to receive encoded and scrambled data signals and process the signals in order to convert them to output stimuli that can be understood by a user of the system, the system comprising:

a data signal decoder for decompressing the data signals;

an output device for generating the output stimuli on the basis of output signals from the decoder;

descrambling means for descrambling the data signals, said descrambling means being activated by an enabling signal; and

enabling means for receiving protected information from a transmitter transmitting the data signals and supplying the enabling signal following the reception of said protective information,

wherein the descrambling means execute a conditional access software program for controlling the descrambling of said data signals, said software program being transported to the descrambling means by the enabling signal.

2. A system as claimed in claim 1, wherein the descrambling means are included in the decoder.

3. A system as claimed in claim 1, wherein the enabling means are included in the decoder.

4. A system as claimed in claim 1, wherein the decoder is included in the output device.

5. A system as claimed in claim 2, wherein the decoder includes an interface to enable data to be exchanged with peripheral equipment, and wherein the conditional access software program is transferred from the enabling means to the descrambling means via the interface by the enabling signal.

6. A system as claimed in claim 1, wherein the enabling means comprise a memory for storing the protected information including said conditional access software program for controlling the descrambling.

7. A system as claimed in claim 1, wherein the enabling means include a detachable memory medium reader, the protected information being stored in a memory of the medium.

8. A system as claimed in claim 7, wherein the detachable memory medium is a chip card.

9. A system as claimed in claim 1, wherein the enabling means are provided with a modem enabling a real-time data exchange between the system and a transmitter of data signals.

10. A method of descrambling and decompressing data signals within a system for converting said signals into output stimuli that can be understood by a user of the system, the method comprising transferring a conditional access software program, from enabling means for receiving protected information from a transmitter of data signals, to descrambling means comprising hardware for executing said software program.